【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 September 2002 (06.09.2002)

PCT

(10) International Publication Number
WO 02/069071 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number: PCT/IB02/00459

(22) International Filing Date: 14 February 2002 (14.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/271,400 26 February 2001 (26.02.2001) US
09/969,004 2 October 2001 (02.10.2001) US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: STARING, Antonius, A., M.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). EPSTEIN, Michael; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: SCHMITZ, Herman, J., R.; International Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

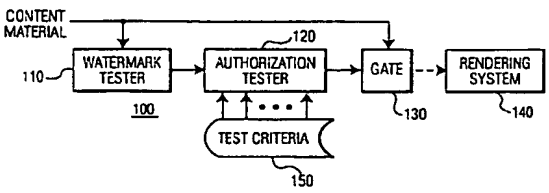
(81) Designated States (*national*): CN, JP, KR.

(84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COPY PROTECTION VIA MULTIPLE TESTS



(57) Abstract: A multi-layered copy protection scheme distinguishes between security failures due to faulty watermark detection schemes and true security failures. At an initial security level, the fault-tolerance is low. If the security test fails at this initial security level, the process enters a next level of security, wherein the fault-tolerance is increased, but at the expense of additional processing time. If the security test again fails at this increased security level, the process enters a higher level of security, wherein the fault-tolerance is further increased, but at the further expense of additional processing time. Eventually, either the security test is passed, and the protected material is rendered, or a determination is made that the failures are not due to faults in the watermark detection process, indicating that the content material is, in fact, copy protected, but not authorized for rendering.

WO 02/069071 A2

Copy protection via multiple tests

This application claims the benefit of U.S. Provisional Application No. 60/271,400, filed 26 February 2001, Attorney Docket US010044P.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of data protection, and in particular to protecting data from illicit copying from a remote location.

2. Description of Related Art

The protection of data is becoming an increasingly important area of security. In many situations, the authority to copy or otherwise process information is verified by evaluating the encoding of copy-protected material for particular characteristics. For example, copy-protected material may contain watermarks or other encodings that identify the material as being copy-protected, and also contains other encodings that identify whether this particular copy of the material is an authorized copy, and whether it can be copied again. For example, an authorized copy of content material may contain a robust watermark and a fragile watermark. The robust watermark is intended to be irremovable from the encoding of the content material. Attempting to remove the watermark causes damage to the content material. The fragile watermark is intended to be damaged when the content material is illicitly copied. For example, common fragile watermarks are damaged if the content material is compressed or otherwise altered. In this manner, content material that is compressed in order to be efficiently communicated via the Internet will be received with a robust watermark and a damaged fragile watermark. A content-processing device that is configured to enforce copy protection rights in this example will be configured to detect the presence of a robust watermark, and prevent the processing of the content material containing this robust watermark unless the fragile watermark is also present.

The design of a watermarking encoding process and corresponding watermark detection involves a tradeoff among conflicting requirements. An ideal watermark should be undetectable during a conventional rendering of the content material, yet easily detectable by

the watermark detector. As the watermark's detectability by the watermark detector increases, so too does its detectability during a conventional rendering; similarly, as the watermark's undetectability during a convention rendering decreases, so too does its undetectability by the watermark detector. Conventional watermarking processes are biased to assure that the watermarking process does not affect the quality of the rendering of the content material, often at the cost of reduced detectability by a watermark detector. That is, the likelihood of a watermark detector producing an erroneous decoding of a watermark is not insubstantial. Given that watermark detection is not absolutely reliable, a need exists for a fault-tolerant watermark-based security process.

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to provide a robust and reliable copy protection scheme in the presence of a potentially unreliable watermark detection process. It is a further object of this invention to provide a copy protection scheme that is fault tolerant.

These objects and other are achieved by a multi-layered copy protection scheme. At an initial security level, the fault-tolerance is low. If the security test fails at this initial security level, the process enters a next level of security, wherein the fault-tolerance is increased, but at the expense of additional processing time. If the security test again fails at this increased security level, the process enters a higher level of security, wherein the fault-tolerance is further increased, but at the further expense of additional processing time. Eventually, either the security test is passed, and the material is rendered, or a determination is made that the failures are not due to faults in the watermark detection process, indicating that the content material is, in fact, copy protected, but not authorized for rendering.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example block diagram of a security system in accordance with this invention.

FIG. 2 illustrates an example flow diagram of a security system in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

A variety of security schemes that are based on the decoding of one or more parameters from a watermark are known in the art, and further watermark-based security schemes can be expected to be developed in the future. Generally, however, these schemes assume that the watermark detection process is reliable, such that, when the watermark detection process reports a result, the security process effects a control based on the reported result.

Because common watermark detection processes are not 100% reliable, a fault in the detection process may be interpreted by the security process as an erroneous watermark, and the rendering of the content material may be inappropriately terminated. That is, the content material may be authorized for rendering, and contain a proper watermark, but the fault in the detection process may indicate an improper watermark, or no watermark. Similarly, but less likely, the content material may be unauthorized, and the fault in the detection process may inappropriately indicate an authorization, or may fail to identify the material as being copy protected.

In accordance with this invention, a multi-level security process is preferably employed to distinguish between faults in the detection process, and truly faulty watermarks.

FIG. 1 illustrates an example block diagram of a security system 100 in accordance with this invention. The system 100 includes a watermark tester 110, and an authorization system 120 that determines whether the input content material is authorized to be rendered, based on information provided by the watermark tester 110. For the purposes of this disclosure, the term "render" includes any subsequent transmission or processing of the input content material, including recording, broadcasting, playing back, converting, and so on. The authorization tester controls a gate 130 that determines whether the content material is presented to a rendering system 140, as indicated by the dashed line between the gate 130 and the rendering system 140.

In accordance with this invention, the authorization tester 120 is configured to accept test criteria 150 for determining whether the information provided by the watermark tester 110 warrants the connection or disconnection of the content material to the rendering system 140. In a conventional security system, the information from a watermark tester 110 is assumed to be reliable and accurate. This invention, on the other hand, is premised on the realization that watermark testers are inherently unreliable and/or inaccurate, due to the purposeful characteristic of the watermark that it not interfere with the rendering process. The

test criteria 150 are specifically formulated to distinguish between a somewhat unreliable watermark tester 110 and an illicit copy of the content material.

Table 1 illustrates a set of example test criteria 150. Initially, at test level 1, a maximum 'test limit' of three watermark tests are conducted. Ideally, these three tests will each report a 'success' if the content material that is being tested has the appropriate watermark, and will each report a 'failure' if the content material that is being tested has a faulty or inappropriate watermark. Recognizing that the watermark testing process may itself be faulty, the test criteria 'fail limit' of table 1 indicates that one failure is acceptable. That is, if the three watermark tests at level 1 indicate two successes and one failure, the authorization tester 120 will declare the content material to be authorized.

Test Level	Test Limit	Fail Limit
1	3	1
2	6	2
3	9	3

Table 1.

If, on the other hand, the test at level 1 indicates more than one failure, the authorization tester 150 enters the next test level, and applies the test limits and failure limits indicated in table 1 for test level 2. At level 2, a maximum of six watermarking tests are conducted. If two or fewer failures occur during these six watermarking tests, the authorization tester 150 will determine that the content material is authorized. If more than two failures occur, the authorization tester 150 enters the next test level, requiring no more than three failures in nine tests. Additional, or fewer, test levels may be included in the test criteria 150. The test procedure continues until the material is determined to be authorized, or until completion of the last test, whichever occurs first. If the last test is completed without a determination that the material is authorized, the material is rejected as being unauthorized.

The particular interpretation of the test criteria may vary, depending upon whether prior tests are intended to affect the determinations at future test levels. That is, for example, the test and failure limits of table 1 may be cumulative limits, or, the test and failure limits of table 1 may be independent for each test level.

In the cumulative example, when a second failure occurs at level 1, the system enters level 2 with a 'history' of the tests of level 1. Thus, because two failures have already occurred, the content material must pass the watermark tests for each subsequent test, until a

total of six tests have been conducted (two or three at level 1 that produced the two failures, then four or three tests at level 2 with no failures). If, during the testing at level 2, a third failure occurs, the system enters level 3, and the content material must pass each of the remaining tests until a total of nine tests have been conducted.

In the independent example, when a second failure occurs at level 1, the system enters level 2, and restarts the testing process, allowing up to two additional failures within six additional tests.

The choice of test criteria, as well as the choice of a cumulative testing process through each level, or an independent testing process at each level, will be made dependent upon an estimate of the likelihood that the watermark tester 110 will report an erroneous result. If the watermark tester 110 rarely reports an erroneous result, the failure limit can be set to a very low value. Conversely, if the watermark tester 110 frequently reports erroneous results, a higher failure limit would be warranted. A cumulative test process will generally result in fewer tests being required, because the results of prior tests are not discarded.

When all of the test levels have been applied and the content material continues to fail each test, the authorization tester 150 will determine that the content material is not authorized, and will control the gate 130 to prevent the communication of the content material to the rendering system 140.

The use of this invention is hereinafter presented in the context of copending U.S. patent application "Protecting Content from Illicit Reproduction by Proof of Existence of a Complete Data Set via Self-Referencing Sections", U.S. serial number 09/536,944, filed 28 March 2000 for Antonius A. M. Staring, Michael A. Epstein, and Martin Rosner, Attorney Docket US000040, incorporated by reference herein. In this copending application, each section of a data set is uniquely identified and this section identifier is encoded as a watermark that is embedded in each section, preferably as a combination of robust and fragile watermarks. When an item of the data set is presented for rendering, the security system requests random sections of the data set, and verifies that the appropriate watermark is present in each of the randomly selected sections. If a sufficient number of randomly selected sections are verified, the entire data set is determined to be present. If the entire data set is not present, the likelihood of randomly selecting an absent section is proportional to the amount of material that is missing from the entire data set. This security scheme is intended to discourage the illicit distribution of select segments of a larger data set.

In the context of digital audio recordings, for example, a compliant playback or recording device is configured to refuse to render an individual song in the absence of verification that the entire contents of the CD is present, via the random watermark testing. The time required to download an entire album on a CD in uncompressed digital form, even at DSL and cable modem speeds, can be expected to be greater than an hour, depending upon network loading and other factors. Thus, by requiring that the entire contents of the CD be present, at a download "cost" of over an hour, the likelihood of a theft of a song via a wide-scale distribution on the Internet is substantially reduced.

In accordance with this invention, the test criteria 150 of FIG. 1 will be determined based upon the degree of security required, and based upon the reliability of the watermark testing process 110. The test limit of table 1 is generally set to assure that a sufficiently large sample of the data set is verified, to assure that the entirety of the data set is present, and the fail limit is set to assure that the test does not result in the rejection of authorized content material due to occasional errors in the watermark testing process 110. The partitioning of the test into multiple levels provides for efficient testing, when it becomes very obvious, based on a low failure rate, that the data set must be present. That is, the lower level tests are preferably structured with a low failure, so that, if the watermarking test is reliable, the test at the lower level ends with an authorization to render the material, if the material is authorized. Time is spent performing the subsequent level tests only if the entirety of the data set is not present, or when a premature rejection of content material is to be avoided.

FIG. 2 illustrates an example flow diagram for a multi-level authorization process in accordance with this invention. At 210, the initial pass/fail test criteria are set, corresponding for example to the first level test of table 1. At 220, a watermark test is conducted, and a pass/fail result is produced.

If the number of failures thus far is below the 'fail limit', at 230, the number of tests conducted thus far is assessed. If, at 240, the number of tests thus far is below the 'test limit', the process loops back to conduct the next watermark test, at 220. Otherwise, if the number of tests conducted thus far equals the test limit, the process terminates with an "authorized" result, at 250.

If the number of failures thus far has reached the 'fail limit', at 230, a determination is made, at 260, as to whether there are additional test levels available. If not, if the terminal tests have been conducted, then the process terminates with a "non-authorized" result, at 270. If, at 260, additional test levels are available, then the next set of test criteria

replaces the prior set of test criteria, at 280, and the process loops back to conduct the next watermark test, at 220. As discussed above, when the next level criteria is loaded, at 280, the prior accumulation of tests and failures is either discarded, for independent test levels, or not discarded, for accumulated test levels.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, the test criteria 150 of FIG. 1 are presented above as a relatively static set of criteria. Adaptive testing may also be conducted, wherein the test criteria at each level is determined based on past performance, or based on external parameters, such as a 'noise figure' or 'quality figure' that may be provided by the watermark tester 110, or other device. The past performance could include a history of errors associated with the watermark tester 110 (e.g. an average number of reported failures for material that was eventually determined to be authorized), wherein the failure limit is dynamically set based on the prior error rate. Additionally, the past performance could include a history of attempted renderings of unauthorized material, wherein the test limit is dynamically set based on the rate of prior authorizations or un-authorizations. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS:

1. A security system (100) for protecting content material, comprising:
a watermark tester (110) that is configured to detect one or more parameters associated with a watermark that is associated with the content material, and
an authorization tester (120), operably coupled to the watermark tester (110), that is configured to determine an authorization corresponding to the content material, based on the one or more parameters detected by the watermark tester (110), and one or more test criteria (150), wherein
the one or more test criteria (150) are based on a likelihood of error associated with the watermark tester (110) in determining the one or more parameters associated with the watermark.

2. The security system (100) of claim 1, wherein
the one or more test criteria (150) includes a set of criteria for each of a plurality of test levels, and
the authorization tester (120) is configured to select a next set of criteria of the plurality of test levels when the authorization tester (120) fails to determine an authorization based on a prior set of criteria of the plurality of test levels.

3. The security system (100) of claim 2, wherein
each set of criteria includes:
a test limit that corresponds to a minimum number of tests that are to be conducted by the watermark tester (110) to determine the authorization, and
a fail limit that corresponds to a maximum number of failures to determine the authorization.

4. The security system (100) of claim 3, wherein
the authorization tester (120) applies the next set of criteria based on results of the watermark tester (110) while applying the prior set of criteria.

5. The security system (100) of claim 3, wherein
the authorization tester (120) applies the next set of criteria independent of results of the watermark tester (110) while applying the prior set of criteria.

6. The security system (100) of claim 1, wherein
the one or more test criteria (150) includes:
a test limit that corresponds to a minimum number of tests that are to be conducted by the watermark tester (110) to determine the authorization, and
a fail limit that corresponds to a maximum number of failures to determine the authorization.

7. The security system (100) of claim 1, wherein
the one or more test criteria (150) includes
a test limit that corresponds to a maximum number of tests that are to be conducted by the watermark tester (110) to reject the content material.

8. The security system (100) of claim 1, wherein
the authorization tester (120) is configured to determine whether an entirety of a data set is present, based on watermarks associated with segments of the data set.

9. The security system (100) of claim 8, wherein
the authorization tester (120) is configured to select a random segment of the data set for testing by the watermark tester (110).

10. A method for protecting content material, comprising:
detecting (220) one or more parameters associated with a watermark that is associated with the content material, and
determining (230-280) an authorization corresponding to the content material, based on the one or more parameters and one or more test criteria (150), wherein
the one or more test criteria (150) are based on a likelihood of error associated with the detecting of the one or more parameters associated with the watermark.

11. The method of claim 10, wherein

the one or more test criteria (150) includes a set of criteria for each of a plurality of test levels, and

determining (230-280) the authorization includes:

selecting (280) a next set of criteria of the plurality of test levels upon failing (230) to determine an authorization based on a prior set of criteria of the plurality of test levels.

12. The method of claim 11, wherein

each set of criteria includes:

a test limit that corresponds to a minimum number of tests that are to be conducted to determine the authorization (240), and

a fail limit that corresponds to a maximum number of failures to determine the authorization (230).

13. The method of claim 11, wherein

determining the authorization based on the next set of criteria includes results while applying the prior set of criteria.

14. The method of claim 11, wherein

determining the authorization based on the next set of criteria is independent of results while applying the prior set of criteria.

15. The method of claim 10, wherein

the one or more test criteria (150) includes:

a test limit that corresponds to a minimum number of tests that are to be conducted to determine the authorization (240), and

a fail limit that corresponds to a maximum number of failures to determine the authorization (230).

16. The method of claim 10, wherein

the one or more test criteria (150) includes

a test limit that corresponds to a maximum number of tests that are to be conducted to reject the content material (260).

17. The method of claim 10, wherein
determining the authorization corresponds to determining whether an entirety of a data set is present, based on watermarks associated with segments of the data set.

18. The method of claim 17, further including
selecting a random segment of the data set.

1/1

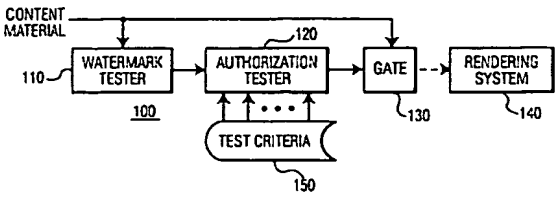

CONTENT MATERIAL
WATERMARK TESTER
110
100
AUTHORIZATION TESTER
120
GATE
130
RENDERING SYSTEM
140
TEST CRITERIA
150

FIG. 1

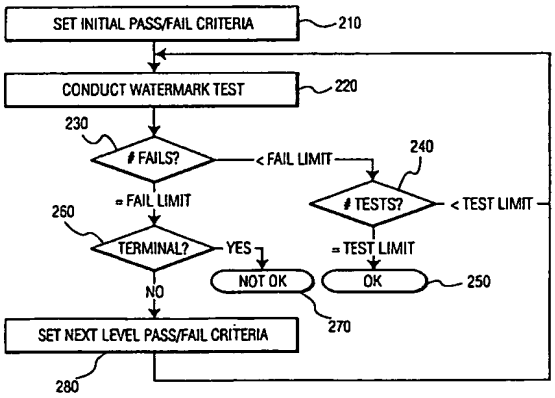

SET INITIAL PASS/FAIL CRITERIA
210
CONDUCT WATERMARK TEST
220
230
FAILS?
< FAIL LIMIT
240
TESTS?
< TEST LIMIT
= FAIL LIMIT
260
TERMINAL?
YES
= TEST LIMIT
NOT OK
OK
250
NO
270
SET NEXT LEVEL PASS/FAIL CRITERIA
280

FIG. 2

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/00459

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G11B G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 12347 A (KONINKL PHILIPS ELECTONICS N V ;PHILIPS SVENSKA AB (SE)) 11 March 1999 (1999-03-11) ABSTRACT page 4, line 7 -page 5, line 13; figure 4	1,8-10, 17,18
P,A	EP 1 096 782 A (CANON KK) 2 May 2001 (2001-05-02) claims 1-6	1,2,10, 11
A	WO 00 75925 A (INTERTRUST TECHNOLOGIES CORP) 14 December 2000 (2000-12-14) page 3, line 15 - line 30	8,9,17, 18

☐ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 June 2003	02/07/2003
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Vellas, E

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 02/03459

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9912347	A	11-03-1999	CN	1246239 T	01-03-2000
			EP	0941605 A1	15-09-1999
			WO	9912347 A2	11-03-1999
			JP	2001505753 T	24-04-2001
			US	6252972 B1	26-06-2001
EP 1096782	A	02-05-2001	JP	2001127976 A	11-05-2001
			EP	1096782 A2	02-05-2001
WO 0075925	A	14-12-2000	AU	5598600 A	28-12-2000
			WO	0075925 A1	14-12-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(74)代理人 100121083
弁理士 青木 宏義
(72)発明者 スタリング アントニウス エイ エム
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6
(72)発明者 エプステイン ミカエル
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6

Fターム(参考) 5B017 AA06 BA09
5J104 AA08 AA12 AA14 PA14